

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California
Corporation,

Plaintiff and
Counterclaim-Defendant,

v.

INTERNET SECURITY SYSTEMS, INC., a
Delaware corporation, INTERNET
SECURITY SYSTEMS, INC., a Georgia
corporation, and SYMANTEC
CORPORATION, a Delaware corporation,

Defendants and
Counterclaim-Plaintiffs.

Civil Action No. 04-CV-1199 (SLR)

PUBLIC VERSION

THIS DOCUMENT CONTAINS
MATERIALS WHICH ARE CLAIMED
TO BE CONFIDENTIAL AND
COVERED BY A PROTECTIVE ORDER.
THIS DOCUMENT SHALL NOT BE
MADE AVAILABLE TO ANY PERSON
OTHER THAN THE COURT AND
OUTSIDE COUNSEL OF RECORD FOR
THE PARTIES)

**DEFENDANTS' JOINT REPLY BRIEF IN SUPPORT OF THEIR
MOTION FOR SUMMARY JUDGMENT OF INVALIDITY
PURSUANT TO 35 U.S.C. §§ 102 & 103**

Richard K. Herrmann (#405)
Morris, James, Hitchens & Williams, LLP
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306
Tel: (302) 888-6800
Fax: (302) 571-1751

*Attorneys for Defendant and Counterclaim
Plaintiff Symantec Corporation*

OF COUNSEL:

Lloyd R. Day, Jr. (*pro hac vice*)
Robert M. Galvin (*pro hac vice*)
Paul S. Grewal (*pro hac vice*)
Day Casebeer Madrid & Batchelder LLP
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop (*pro hac vice*)

Symantec Corporation

20330 Stevens Creek Blvd.

Cupertino, CA 95014

Tel: (408) 517-8000

Fax: (408) 517-8121

Dated: July 10, 2006

Redaction Date: July 19, 2006

Table of Contents

	Page No.
I. INTRODUCTION.....	1
II. SUMMARY JUDGMENT OF INVALIDITY SHOULD BE ENTERED ON ALL OF THE ASSERTED CLAIMS	2
A. LEGAL STANDARDS	2
B. EMERALD 1997 ANTICIPATES AND RENDERS OBVIOUS THE ASSERTED CLAIMS	2
1. Emerald 1997 anticipates the claimed inventions of the '212 patent.....	3
2. Emerald 1997 inherently anticipates all of the asserted claims of the '203 and '615 patents	6
3. Emerald 1997 and Intrusive Activity 1991 render the '203 and '615 claims obvious.....	8
C. THE LIVE TRAFFIC PUBLICATION ANTICIPATES THE ASSERTED CLAIMS	14
D. THE JINAO REPORT ANTICIPATES THE ASSERTED CLAIMS	14
1. The JiNao Report anticipates the asserted '338 claims	15
2. The JiNao Report anticipates the asserted hierarchical claims.....	17
III.CONCLUSION	20

TABLE OF AUTHORITIES

	PAGE NO.
Cases	
<i>Akamai Techs. v. Cable & Wireless Internet Servs.,</i> 344 F.3d 1186, 1192 (Fed. Cir. 2003).....	6
<i>Bristol-Myers Squibb Co. v. Ben Venue Labs., Inc.,</i> 246 F.3d 1368, 1379 (Fed. Cir. 2001).....	19
<i>Ferring B.V. v. Barr Labs., Inc.,</i> 437 F.3d 1181, 1193 (Fed. Cir. 2006).....	8
<i>In re Cronyn,</i> 890 F.2d 1158, 1159 (Fed. Cir. 1989).....	14
<i>In re Donohue,</i> 766 F.2d 531, 533 (Fed. Cir. 1985).....	19
<i>In re Kahn,</i> 441 F.3d 977, 988 (Fed. Cir. 2006).....	9
<i>Matsushita Elec. Indus. Co. v. Cinram Int'l, Inc.,</i> 299 F. Supp. 2d 348, 357 (D. Del. 2004).....	2
<i>Motorola, Inc. v. Interdigital Tech. Corp.,</i> 121 F.3d 1461, 1472 (Fed. Cir. 1997).....	13
<i>National Steel Car, Ltd., v. Canadian Pacific Railway, Ltd.,</i> 357 F.3d 1319, 1337 (Fed. Cir. 2004).....	10
<i>Newell Cos. v. Kenney Mfg. Co.,</i> 864 F.2d 757, 763 (Fed. Cir. 1988).....	12
<i>Novo Nordisk Pharma., Inc., v. Bio-Tech. General Corp.,</i> 424 F.3d 1347, 1355 (Fed. Cir. 2005).....	19
<i>Novo Nordisk Pharma., Inc., v. Bio-Tech. General Corp.,</i> Civ. No. 02-332-SLR, 2004 U.S. Dist. LEXIS 14960 at *83 (D. Del. 2004) <i>aff'd in part and vacated in part</i> , 424 F.3d 1347 (Fed. Cir. 2005)	3
<i>Richardson-Vicks Inc. v. Upjohn Co.,</i> 122 F.3d 1476, 1483 (Fed. Cir. 1997).....	13
<i>Ryko Mfg. Co. v. Nu-Star, Inc.,</i> 950 F.2d 714, 719 (Fed. Cir. 1991).....	12

<i>Sandt Tech., Ltd. v. Resco Metal & Plastics Corp.,</i> 264 F.3d 1344, 1355 (Fed. Cir. 2001).....	12
<i>Sewall v. Walters,</i> 21 F.3d 411, 415 (Fed. Cir. 1994).....	4
<i>Union Carbide Corp. v. American Can Co.,</i> 724 F.2d 1567, 1576 (Fed. Cir. 1984).....	12
<i>WMS Gaming Inc. v. Int'l Game Tech.,</i> 184 F.3d 1339, 1355 (Fed. Cir. 1999).....	2

I. INTRODUCTION

Based upon SRI's Answering Brief, very few issues remain in dispute with regard to the prior art at issue: *Emerald 1997*, *Live Traffic*, and *JiNao Report*. For each reference, SRI has conceded disclosure of most or all of the limitations of the claims necessary to find anticipation, and on the remaining points, SRI has not raised a genuine issue of material fact because they have not come forward with evidence sufficient for a reasonable trier of fact to find in its favor, even giving SRI the benefit of all reasonable inferences.

The uncontested issues and SRI's few remaining challenges are summarized below. Defendants have shown there is no genuine issue of material fact that would preclude summary judgment on all asserted claims. At a minimum, partial summary judgment of the following should be granted, which will significantly narrow the issues for trial.

1. *Emerald 1997* discloses all of the limitations of the '212 claims.
 - SRI contests only enablement.
2. *Emerald 1997* discloses all but one of the limitations of the '203 and '615 claims.
 - SRI contests only the disclosure of the claimed "network traffic data" categories. But SRI fails to address Defendants' central inherency argument that *Emerald 1997* discloses directly monitoring network infrastructure such as firewalls.
 - A. *Intrusive Activity 1991* discloses at least one of the claimed network traffic data categories: network packet data volume. Thus, the combination of *Intrusive Activity 1991* and *Emerald 1997* discloses all of the limitations of the '203 and '615 claims.
 - SRI contests only whether network connection requests and denials are also disclosed. SRI does not rebut the disclosure of network packet data volume.
 - B. SRI's expert Dr. Kesidis admitted that *Emerald 1997* provides a motivation to combine *Intrusive Activity 1991*.
 - SRI has not attempted to rebut this admission and instead only claims that secondary considerations trump this primary consideration.
3. *Live Traffic* discloses all of the limitations of all of the claims-in-suit.
 - SRI contests only whether this reference was "publicly available."

4. *JiNao Report* discloses all but one of the limitations of the '338 claims.
 - SRI contests only the limitations "receiving network packets" and "from at least one measure of the network packets" which SRI concedes are synonymous, *i.e.*, if one is disclosed, both are disclosed.
5. *JiNao Report* discloses all but one of the limitations of the '203, '212 and '615 claims.
 - SRI contests whether *JiNao Report* discloses "analysis of network traffic data."
 - With regard to the "automatically receiving... by one or more hierarchical monitors" limitation, SRI raises only an enablement challenge.

II. SUMMARY JUDGMENT OF INVALIDITY SHOULD BE ENTERED ON ALL OF THE ASSERTED CLAIMS

A. LEGAL STANDARDS

Summary judgment is appropriate here because SRI has failed to come forward with specific material facts showing a genuine issue for trial. "Facts that could alter the outcome are material, and disputes are genuine if evidence exists from which a rational person could conclude that the position of the person with the burden of proof on the disputed issue is correct."

Matsushita Elec. Indus. Co. v. Cinram Int'l, Inc., 299 F. Supp. 2d 348, 357 (D. Del. 2004) (citations omitted).

B. EMERALD 1997 ANTICIPATES AND RENDERS OBVIOUS THE ASSERTED CLAIMS

SRI concedes that *Emerald 1997* discloses all of the limitations of the '212 claims, and relies only on a vague "enablement" challenge. SRI also concedes that *Emerald 1997* explicitly discloses all but one of the limitations of the '203 and '615 claims, and challenges only the disclosure of the claimed "network traffic data" categories.

Given these admissions from SRI, its attempt to hide behind the presumption of validity makes no sense. The presumption of validity when a reference has been considered by the Examiner is rebuttable. *WMS Gaming Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1355 (Fed. Cir. 1999). Defendants have overcome the presumption of validity, particularly in this case, where SRI has already *admitted* *Emerald 1997* discloses all of the limitations of the '212, and all but

one of the limitations of the '203 and '615 patents.

As will be shown below, for the few issues SRI contests, Defendants have put forward clear and convincing evidence of invalidity, and SRI has failed to rebut it.¹

1. Emerald 1997 anticipates the claimed inventions of the '212 patent

SRI, conceding that *Emerald 1997* discloses each of the limitations of the '212 claims, relies only on enablement for its claim that *Emerald 1997* does not anticipate the '212 patent claims. Prior art references, including technical publications, are presumed to be enabling. *Novo Nordisk Pharma., Inc., v. Bio-Tech. General Corp.*, Civ. No. 02-332-SLR, 2004 U.S. Dist. LEXIS 14960 at *83 (D. Del. 2004) *aff'd in part and vacated in part*, 424 F.3d 1347 (Fed. Cir. 2005). The patentee bears the burden to show that the prior art reference is not enabled. *Id.* at *73. SRI has not met its burden.²

SRI begins its enablement challenge by mischaracterizing *Emerald 1997* as an "early overview paper."³ This is simply untrue. In fact, *Emerald 1997* was published in October 1997, *some 10 months after* the inventor Mr. Porras published an EMERALD conceptual overview. See P. Porras and P. Neumann, *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances Conceptual Overview*, Dec. 18, 1996.⁴ Furthermore, *Emerald 1997* was published some five months *after* SRI's claimed May 3, 1997 conception date for claim 1 of all four patents.⁵ The latest conception date SRI has claimed for any of the claims is

¹ SRI has also failed to rebut Defendants' evidence that the Examiner in this instance failed to follow the MPEP and did not consider *Emerald 1997* during prosecution of the '203 patent. SRI cites nothing from the actual file history. *See* Opening Br. at 23 [D.I. 299], Res. Br. at 6-7 [D.I. 339].

² Based on undisputed facts, Defendants have carried the burden of showing *Emerald 1997* was enabled, even if it was Defendants' burden, which it is not.

³ Res. Br. at 5-6 [D.I. 339].

⁴ D.I. 301, Ex. JJ.

⁵ SRI's Second Supplemental Responses to Symantec's First Set of Interrogatories [Nos. 1-12] No. 4 [Declaration of Geoffrey M. Godfrey In Support of Defendant's Joint Reply Motion for

October 1, 1997.⁶ An invention that has been conceived is enabled:

Conception exists when a definite and permanent idea of an operative invention, including every feature of the subject matter sought to be patented, is known... Conception is complete when one of ordinary skill in the art could construct the apparatus without unduly extensive research or experimentation.

Sewall v. Walters, 21 F.3d 411, 415 (Fed. Cir. 1994). SRI's claim that “[t]he research proposed in EMERALD 1997 *eventually* led to the conception and reduction to practice of the claimed inventions” is directly contradicted by SRI's own timeline of conception.⁷

SRI challenges only the enablement of the limitation “wherein at least one of the network monitors utilizes a statistical detection method.”⁸ SRI continues its game of attempting to challenge *Emerald 1997* as non-enabled, while maintaining that its patents are enabled. For example, Defendants submitted an exhibit highlighting the similarities between *Emerald 1997* and the patent specification.⁹ SRI has claimed that this exhibit demonstrates that “critical disclosure” is missing from *Emerald 1997*.¹⁰ But SRI points to nothing – not a single sentence – that appears in the patents but does not appear in *Emerald 1997* to support its theory that *Emerald 1997* fails to enable a “statistical detection method.” SRI cannot defeat summary judgment merely by claiming a fact is challenged.

Emerald 1997 devotes an entire section to describing “Scalable Profile-Based Anomaly Detection.” *Emerald 1997* at 359.¹¹ Mr. Valdes, contrary to SRI's claims,¹² expressly admitted

Summary Judgment Regarding Invalidity (“7/10/06 Godfrey Decl.”) Ex. QQ].

⁶ *Id.*; *see also* Porras 30(b)(6) Tr. 140-42 [7/10/06 Godfrey Decl. Ex. RR].

⁷ Res. Br. at 6 (emphasis added) [D.I. 339]; even considering Mr. Porras' testimony that he wrote *Emerald 1997* in approximately July or August 1997, this paper was still written months after conception of the inventions. Porras Tr. 422 [7/10/06 Godfrey Decl. Ex. RR].

⁸ Res. Br. at 14-16 [D.I. 339].

⁹ Brown Decl. Ex. W [D.I. 301].

¹⁰ Res. Br. at 2 [D.I. 339].

¹¹ D.I. 301, Ex. E.

¹² Res. Br. at 15-16 [D.I. 339].

that this section discussed statistical profiling.¹³

In this section, *Emerald 1997* explains that the EMERALD statistical profiling engines use the NIDES statistical algorithms, which are “well suited to the problem of network anomaly detection, with some adaptation.” *Emerald 1997* at 359.¹⁴ *Emerald 1997* then describes certain changes to make to the algorithms for the application to network traffic. *Id.* Not coincidentally, this section explaining the necessary changes appears almost verbatim in the patent specification.¹⁵

Thus, contrary to SRI’s arguments, the *Emerald 1997* paper expressly discussed the modifications to make to the NIDES algorithms. Moreover, SRI’s claim that the NIDES algorithms were not capable of being used for EMERALD *directly contradicts the patent specification itself*, which states:

The profile engine 22 may use a statistical analysis technique described in A. Valdes and D. Anderson, “Statistical Methods for Computer Usage Anomaly Detection using NIDES”, Proceedings of the Third International Workshop on Rough Sets and Soft Computing, January 1995, which is incorporated by reference in its entirety. Such an engine 22 can profile network activity via one or more variables called measures. Measures can be categorized into four classes: categorical, continuous, intensity, and event distribution measures.¹⁶

The patent specification then goes on to discuss these four classes of measures – which are exactly the same measures used in NIDES. *See Statistical Methods* at 307.¹⁷

This description more than enables the statistical detection method of the ‘212 claims to one of ordinary skill in the art, especially in light of the fact that SRI’s witnesses have admitted

¹³ Valdes Tr. 450-51 [7/10/06 Godfrey Decl. Ex. TT].

¹⁴ D.I. 301, Ex. E.

¹⁵ *See* Brown Decl. Ex. W [D.I. 301], ‘338 col. 7:4-15.

¹⁶ ‘338 col. 5:42-52. Note that SRI has admitted that the contents of the referenced paper itself (*Statistical Methods*) is not “essential material” and is not necessary for enablement. *See* Opening Br. at note 21 [D.I. 299]. Thus the algorithms for NIDES disclosed in *Statistical Methods* are not required to enable the claims.

¹⁷ D.I. 301, Ex. FF.

that (1) the inventors were not the first to use a statistical detection method on network traffic,¹⁸ and (2) generic statistical detection techniques that could be applied to network packet data *were known* to those of ordinary skill in October of 1997.¹⁹

SRI has failed to raise a genuine issue of material fact to rebut its burden of proving that *Emerald 1997* is not enabled.

2. Emerald 1997 inherently anticipates all of the asserted claims of the '203 and '615 patents

SRI concedes that all of the '203 and '615 claim limitations except one – the disclosure of the network traffic data categories – are disclosed in *Emerald 1997*. SRI does not contest that *Emerald 1997* discloses monitoring network traffic data generally. Furthermore, SRI fails to even address Defendant's central argument regarding inherent anticipation, let alone raise a genuine issue of material fact.

As it did in its own motion for summary judgment, SRI both misstates the standard for inherent anticipation, and misstates Defendants' arguments. SRI claims that in order to inherently anticipate, it must be shown that a person of ordinary skill in the art would “*necessarily* construct a system” which met the limitations of the claims.²⁰ But the focus of the inherency inquiry is not a requirement of actual construction. The proper legal standard for inherency is met when the prior art reference describes and enables an embodiment which necessarily includes the claimed subject matter. *See Akamai Techs. v. Cable & Wireless Internet Servs.*, 344 F.3d 1186, 1192 (Fed. Cir. 2003). The focus must remain on what the reference discloses.

SRI simply refuses to acknowledge that *Emerald 1997* discloses and teaches monitoring

¹⁸ Kesidis Tr. 380-81 [7/10/06 Godfrey Decl. Ex. SS]; Porras Tr. 335-36 [7/10/06 Godfrey Decl. Ex. RR].

¹⁹ Kesidis Tr. 705 [7/10/06 Godfrey Decl. Ex. SS].

network infrastructure such as firewalls. In fact, by reading SRI's motion, one might think *Emerald 1997* did not even mention network infrastructure and firewalls. But of course, that is not the case. *Emerald 1997* directly teaches monitoring network traffic at firewalls. At the beginning of *Emerald 1997*, the authors explained that one of the problems that they were trying to solve was how to extend techniques that had been developed to monitor centralized computing resources to "cover spatially distributed components such as network *infrastructure* (e.g., routers, filters, DNS, *firewalls*)."²⁰ *Emerald 1997* at 354.²¹ The authors of *Emerald 1997* then described that their solution involved deploying monitors to directly analyze such infrastructure: "Service monitors are dynamically deployed within a domain to provide localized real-time analysis of *infrastructure* (e.g., routers or gateways)" *Emerald 1997* at 355.²² Thus, despite SRI's efforts to ignore this disclosure in the reference, *Emerald 1997* disclosed an embodiment of a service monitor (a network monitor) directly monitoring a firewall.

Given that SRI's Response Brief never even addresses this argument, SRI has failed to raise a genuine issue of material fact. SRI simply ignores the explicit language in *Emerald 1997* teaching monitoring network infrastructure like firewalls. Nor does SRI even attempt to claim that any firewalls existed that did not allow certain packets into the network while blocking others – because this is the very essence of a firewall. Furthermore, SRI does not contest that discarded traffic from a firewall constitutes "network connection denials" and pass-through traffic from a firewall constitutes "network connection requests." By its silence on all these issues, SRI has failed to raise a genuine issue of material fact that *Emerald 1997* did not inherently disclose monitoring network connection requests and denials.

SRI's arguments regarding application logs and mischaracterization of Mr. Avolio's

²⁰ Res. Br. at 7 [D.I. 339].

²¹ D.I. 301, Ex. E.

testimony have already been addressed in Defendants' Joint Opposition to SRI's Motion for Partial Summary Judgment of No Anticipation by the "Emerald 1997" Publication, and for brevity those pleadings are incorporated by reference herein.²³ Despite its arguments in two briefs that not all firewalls kept logs, SRI has failed to put forward any evidence of a single firewall that did not monitor and log network connection requests, network connection denials, and network traffic data volume in the relevant timeframe.

Thus, SRI's argument simply states that facts are challenged without bringing forward any evidence to the contrary. Under well-established law, this fails to raise a genuine issue of material fact that would defeat Defendants' motion. *Ferring B.V. v. Barr Labs., Inc.*, 437 F.3d 1181, 1193 (Fed. Cir. 2006).

3. Emerald 1997 and Intrusive Activity 1991 render the '203 and '615 claims obvious

The combination of *Emerald 1997* and *Intrusive Activity 1991* renders obvious the claims-in-suit of the '203 and '615 patents. *Intrusive Activity 1991*.²⁴ SRI has failed to raise any genuine issues of material fact to the contrary. First, SRI has not contested that *Intrusive Activity 1991* discloses monitoring network traffic data volume, one of the claimed network traffic data categories. SRI also fails to put forth the correct standard for a motivation to combine references. Under the correct standard, SRI's expert has admitted there was motivation to combine *Emerald 1997* and *Intrusive Activity 1991*, a point that SRI does not contest.²⁵ SRI's argument thus reduces to reliance upon secondary considerations of nonobviousness to avoid summary judgment. But the law is clear that secondary considerations do not preclude summary

²² D.I. 301, Ex. E.

²³ D.I. 342.

²⁴ D.I. 301, Ex. F. Despite the fact that one of the inventors cited *Intrusive Activity 1991* in the *Emerald 1997* publication, this reference was never disclosed to the Examiner. Thus, the Examiner never considered this particular obviousness combination.

judgment in this instance.

First, SRI's Response Brief fails to even attempt to rebut that *Intrusive Activity 1991* discloses network packet data volume. The relevant disclosure is clearly called out in Defendants' Opening Brief, which states “[t]wo parameters explicitly called out are ‘the number of packets’ and the ‘number of bytes’ – both of which constitute a measure of ‘network packet data volume.’”²⁶ Through its silence, SRI has implicitly admitted that *Intrusive Activity 1991* discloses monitoring “network packet data volume.” Because disclosure of even one of the claimed categories of network traffic data is sufficient, SRI's silence means that it has conceded that all of the limitations of the ‘203 and ‘615 claims-at-issue are disclosed by the combination of *Emerald 1997* and *Intrusive Activity 1991*.²⁷

SRI also attempts to argue that there was no motivation to combine *Intrusive Activity 1991* with *Emerald 1997*. SRI does not state the actual standard for motivation to combine, but instead appears to conflate it with the anticipation standard for incorporation by reference. For example, SRI states that “[a] person of ordinary skill attempting to practice the disclosure of *EMERALD 1997* would not be required to consult the *Intrusive Activity 1991* article.”²⁸ That is far different from the actual standard for motivation to combine:

²⁵ See *infra* note 33 and accompanying text.

²⁶ Opening Br. at 31 [D.I. 299].

²⁷ SRI instead expends its energy only on attempting to demonstrate that additional disclosures in *Intrusive Activity 1991* do not disclose monitoring “network connection requests” and “network connection denials.” SRI argues, without pointing to any support in the reference itself, that the Network Security Monitor (NSM), the system disclosed in *Intrusive Activity 1991*, only monitored “established connections.” Res. Br. at 13 [D.I. 339]. But SRI's own expert has already disclaimed this argument in his deposition. When questioned, Dr. Kesidis was unable to point to any support for the notion that NSM monitored only established connections. Kesidis Tr. 619-37 at 629, 636-37 [7/10/06 Godfrey Decl. Ex. SS]. In any event, even if SRI had raised a genuine issue of material fact as to whether or not *Intrusive Activity 1991* discloses network connection requests and denials (which it has not) this is irrelevant in light of the fact that SRI has implicitly conceded that the reference discloses monitoring network packet data volume.

²⁸ Res. Br. at 12 [D.I. 339].

[W]hether a person of ordinary skill in the art, possessed with the understandings and knowledge reflected in the prior art, and motivated by the general problem facing the inventor, would have been led to make the combination recited in the claims.

In re Kahn, 441 F.3d 977, 988 (Fed. Cir. 2006).

While an explicit motivation to combine is not required, here Defendants have actually demonstrated such an explicit motivation in the *Emerald 1997* reference itself. *National Steel Car, Ltd., v. Canadian Pacific Railway, Ltd.*, 357 F.3d 1319, 1337 (Fed. Cir. 2004). The text of *Emerald 1997* states the *Intrusive Activity 1991* article relates to “analyz[ing] packet data” and further provides a citation to *Intrusive Activity 1991*.²⁹ *Emerald 1997* disclosed that network packets were a source of event data for the EMERALD system, and thus one of ordinary skill interested in learning more about how EMERALD performed network packet data monitoring would have been motivated to combine the teachings of *Intrusive Activity 1991*.³⁰

SRI’s expert *agreed at his deposition* that these facts established a motivation to combine the two references:

REDACTED

SRI never even mentions or discusses this admission from their own expert.

Instead, SRI attempts to distinguish *Application of Saunders*, 444 F.2d 599, 601 (C.C.P.A. 1971) from the situation at issue. SRI appears to suggest that because *Saunders* dealt with patents, and the references in this case are technical papers, somehow *Saunders* is

²⁹ See *Emerald 1997* at 364 and 365[7] [D.I. 301, Ex. E].

³⁰ See *Emerald 1997* at 356 [D.I. 301, Ex. E]. See also Kesidis Tr. 670-72 (admitting a network datagram is equivalent to a packet) [D.I. 301, Ex. V].

³¹ Kesidis Tr. 675-76 [D.I. 301, Ex. V]; see also Porras Tr. 424-25 [7/10/06 Godfrey Decl. Ex.

irrelevant. SRI also appears to conflate a finding of a motivation to combine with the standard for incorporation by reference.³² But Defendants merely cited to *In re Saunders* for the unsurprising notion that it is obvious to combine references where a first reference points to a second reference explicitly. SRI's analysis of minute distinctions between *Saunders* and the current situation do nothing to cast doubt upon this general concept. Indeed, as noted above, both SRI's expert and one of the inventors agreed that the facts in this case establish a motivation to combine the two references.³³

The only additional argument made by SRI is that "there would be no motivation to consult such an outdated technical article in a rapidly evolving field such as network security."³⁴ SRI cites no law for the proposition that motivation to combine depends upon the age of a reference. Furthermore, *Intrusive Activity 1991* was not an "outdated" reference – it described NSM, the well-known earliest network intrusion detection system.³⁵ NSM has been widely acknowledged as groundbreaking work.³⁶ This argument by SRI only draws attention to the fact that monitoring the claimed network traffic categories was old – quite old, as *Intrusive Activity 1991* demonstrates, and as the inventors themselves have admitted.³⁷ It is unsurprising that the authors of *Emerald 1997* would cite to a reference describing one of the seminal works on network intrusion detection to provide further information on specific network traffic categories

RR].

³² Res. Br. at 10-12 [D.I. 339].

³³ Kesidis Tr. 675-76 [D.I. 301, Ex. V]; *see also* Porras Tr. 424-25 [7/10/06 Godfrey Decl. Ex. RR].

³⁴ Res. Br. at 12 [D.I. 339].

³⁵ Porras Tr. 241-43 [7/10/06 Godfrey Decl. Ex. RR].

³⁶ *See, e.g.*, R. Bace, INTRUSION DETECTION at 19-20 (stating "NSM was a significant milestone in intrusion detection research because it was the first attempt to extend intrusion detection to heterogeneous network environments.") [7/10/06 Godfrey Decl. Ex. YY].

³⁷ Porras Tr. 289-95, 444-54 [D.I. 301, Ex. T]; Valdes Tr. 283-87 [D.I. 301, Ex. U]; *see also* discussion in Defendant's Joint Opposition to SRI's Motion for Partial Summary Judgment of No Anticipation by the "EMERALD 1997" Publication at 10-11 [D.I. 342].

to monitor.

SRI's failure to rebut the concession from their own expert that *Emerald 1997* provides an explicit motivation to combine *Intrusive Activity 1991* demonstrates that SRI has failed to raise a genuine issue of material fact regarding motivation to combine.

a. SRI's "Evidence" of Secondary Considerations Does Not Preclude Summary Judgment

SRI also claims that evidence of "secondary considerations" (put forth by their expert) is sufficient to preclude summary judgment.³⁸ But this is not the law, even if the Court accepts all of these alleged facts in a light most favorable to SRI.³⁹ Summary judgment of obviousness is often appropriate even if the plaintiff presents evidence of secondary considerations of nonobviousness. *See Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 719 (Fed. Cir. 1991) (upholding summary judgment of obviousness where, although "secondary considerations weighed in favor of [patent owner]," summary judgment still was appropriate because "[t]he district court determined that secondary considerations did not carry sufficient weight to override a determination of obviousness based on primary considerations"); *Sandt Tech., Ltd. v. Resco Metal & Plastics Corp.*, 264 F.3d 1344, 1355 (Fed. Cir. 2001) (upholding summary judgment of obviousness and noting that "[w]e see no error in the district court's conclusion in this case that the secondary considerations cannot overcome the strong evidence of obviousness presented."); *see also Union Carbide Corp. v. American Can Co.*, 724 F.2d 1567, 1576 (Fed. Cir. 1984).

Here, what the parties dispute is the *ultimate legal conclusion of obviousness*, not the underlying facts. Accordingly, there is no issue of fact requiring a trial:

[W]here the ultimate legal conclusion of obviousness is disputed, but not the

³⁸ Res. Br. at 30-31 [D.I. 339].

³⁹ Defendants do not present their disputes on these positions in this motion because the secondary considerations do not affect the outcome of the ultimate legal conclusion of obviousness.

underlying facts, there is no issue of fact requiring a trial, even though some facts favor obviousness, some nonobviousness. This is so even in a case where a jury is demanded, because it is not the function of the jury to pick and choose among *established facts* relating to obviousness in contrast to its obligation to sift through *conflicting evidence* and determine what those facts are.

Newell Cos. v. Kenney Mfg. Co., 864 F.2d 757, 763 (Fed. Cir. 1988) (internal citations omitted).

The existence of evidence of secondary considerations “does not control the obviousness determination.” *Richardson-Vicks Inc. v. Upjohn Co.*, 122 F.3d 1476, 1483 (Fed. Cir. 1997) (upholding summary judgment of obviousness in part because “[t]he unexpected results and commercial success of the claimed invention, although supported by substantial evidence, do not overcome the clear and convincing evidence that the subject matter sought to be patented is obvious”); *see also Motorola, Inc. v. Interdigital Tech. Corp.*, 121 F.3d 1461, 1472 (Fed. Cir. 1997). Here, the “secondary considerations cannot overcome the strong evidence of obviousness.” *Sandt Tech.*, 264 F.3d at 1355. Indeed, SRI makes no attempt to explain why any of these secondary considerations would affect the explicit motivation to combine the references.

As SRI’s expert conceded, *Emerald 1997* itself provides an express motivation to combine its teachings with the teachings of *Intrusive Activity 1991*.⁴⁰ Given this admitted express motivation to combine within SRI’s own publication, summary judgment of invalidity under § 103 is appropriate.⁴¹

⁴⁰ Kesidis Tr. 673-76 [D.I. 301, Ex. V].

⁴¹ SRI’s behavior in discovery regarding secondary considerations should also prevent them from benefiting from such “facts.” During fact discovery, SRI maintained in its Interrogatory Responses that Peter Neumann was the SRI employee most knowledgeable about secondary considerations. *See* SRI’s Supplemental Response to Interrogatories No. 12 and No. 15 [No. 12], dated Dec. 15, 2005 (identifying Peter Neumann at page 2). [7/10/06 Godfrey Decl. Ex. WW]. But at his deposition on the last day of fact discovery, Mr. Neumann disclaimed all knowledge of any secondary considerations. Neumann Tr. 147-59 [7/10/06 Godfrey Decl. Ex. VV]. Only over a month *after* the close of fact discovery did SRI supplement its Interrogatory Responses and remove Mr. Neumann’s name as the person most knowledgeable. *See* SRI’s Supplemental Response to Symantec’s Interrogatories Nos. 1, 12 (First Set of Interrogatories), 13 and 15 (Second Set of Interrogatories) [No. 12], dated May 5, 2006 (identifying Phillip

C. THE LIVE TRAFFIC PUBLICATION ANTICIPATES THE ASSERTED CLAIMS

SRI does not challenge the fact that *Live Traffic* anticipates *all* of the claims-at-issue. In addition, SRI has not put forward any facts of its own contesting Defendants' showing that the *Live Traffic* paper was posted on both SRI's FTP site and SRI's WWW website prior to the 35 U.S.C. § 102(b) critical date.⁴² Nor has SRI put forward any facts contesting the actual contents of the version of *Live Traffic* that was posted to the FTP and WWW websites. Defendants' factual showing on these issues is laid out in their Opening Brief, as well as Defendants' Answering Brief to SRI's Motion for Partial Summary Judgment that the Live Traffic Article is Not a Section 102(b) Printed Publication,⁴³ which are respectfully incorporated herein.

The only challenge SRI has raised is whether or not the above facts render *Live Traffic* "publicly available." "[W]here there are no disputed factual issues, the question whether particular material is a 'printed publication' is a question of law." *In re Cronyn*, 890 F.2d 1158, 1159 (Fed. Cir. 1989). Defendants' legal arguments have already been laid out in the previously-referenced briefs, and demonstrate that both the FTP and WWW *Live Traffic* postings satisfy the standard for a "publicly available" reference. Thus, this issue is appropriate for summary judgment in Defendants' favor.

D. THE JINAO REPORT ANTICIPATES THE ASSERTED CLAIMS

SRI purports to contest *JiNao Report*'s disclosure of only one of the limitations of the '338 claims, and only one of the limitations of the '203, '212, and '615 ("hierarchical") claims. As explained in detail below, the rest of SRI's arguments, while styled as challenging the "disclosure" of an additional limitation of the hierarchical patents, are actually enablement arguments.

⁴² Porras as the person most knowledgeable at page 4). [7/10/06 Godfrey Decl. Ex. XX].

⁴³ Defendants withdraw their claims regarding *Live Traffic* and 35 U.S.C. § 102(a).

1. The JiNao Report anticipates the asserted '338 claims

The only limitation of the '338 claims that SRI alleges is not disclosed by the *JiNao Report* is building statistical profiles "from at least one measure of the network packets."⁴⁴ As support for this proposition, SRI attempts to suggest that JiNao used audit records, rather than network packets, as its data source. But *JiNao Report* repeatedly discloses that "measures" are built from network packets. The JiNao authors characterized one type of these network packet measures as an "audit record distribution measure" because JiNao used the NIDES algorithms, and this was the name of one of the four measures used in NIDES.⁴⁵ This does not change the fact, however, that the *JiNao Report* clearly discloses analysis of network traffic and network packets, and the creation of statistical profiles based upon received packets.

SRI claims that the JiNao system was akin to the "early systems focused on the analysis of audit logs."⁴⁶ But the introduction of the *JiNao Report* specifically distinguishes JiNao from analysis of host audit trails and explains that JiNao *looks at network traffic*:

In the early stage, intrusion detection system [sic] were designed around the analysis of a single host's audit trail. With the proliferation of computer networks, many of the intrusion detection systems began to extend the techniques to networks of computers. Most of the current network intrusion detection efforts have taken one of the two following approaches. One approach is to collect data from separate hosts on a network for processing by a centralized intrusion detection system [2][3]. The other approach is to target network traffic at the service and protocol levels [6][7]. Our effort is close to the second approach with a few exceptions. First we are interested in protecting network infrastructure and particularly focus on routing and management capabilities. Therefore, the target of analysis is mainly on specific protocol traffic instead of general data traffic.⁴⁷

The *JiNao Report* states that JiNao *receives* network packets and uses them to create measures:

⁴³ D.I. 367.

⁴⁴ Res. Br. at 25 [D.I. 339]. SRI treats the additional limitation of "receiving network packets" as synonymous with this limitation. Res. Br. at 27 [D.I. 339].

⁴⁵ See *Statistical Methods* at 307 (stating "NIDES uses four classes of measures: activity intensity, audit record distribution, categorical, and continuous.") [D.I. 301, Ex. FF].

⁴⁶ Res. Br. at 26 [D.I. 339].

Measures: Aspects of subject behavior are represented as measures (e.g., *packet* and LSA arrival frequencies in terms of their types or sources). For each measure, we will construct a probability distribution of short-term and long-term behaviors. For example, *for the packet types received, the long-term probability distribution would consist of the historical probabilities with which different types of packets have been received*, and the short-term probability distribution would consist of the recent probabilities *with which different types of packets have been received*.⁴⁸

The *JiNao Report* discusses packets and the receipt of packets repeatedly.⁴⁹

The *JiNao Report* explains that for purposes of applying the NIDES algorithms, these measures based upon received packets are *classified* into different categories taken from the NIDES algorithms:

In this case, the categories to which probabilities are attached are the names of packet types, which are learned by the system as they are received. *We would classify the Ji-Nao measures into two groups*: activity intensity and audit record distribution measures.⁵⁰

Even the mathematical formulae for computing the “audit record distribution measures” makes it clear that this measure is built using received packets. *See JiNao Report* at 21 (“ $W_{m,j}$ is the number of packets received on the j^{th} day...”)⁵¹ *See also* the Declaration of L. Todd Heberlein for further explanation of the use of the term “audit” in the intrusion detection field.⁵²

SRI’s expert’s attempt to distinguish JiNao as merely “reacting” to network packets strains all credibility and fails to raise a *genuine* issue of material fact. Even Dr. Kesidis himself

⁴⁷ *JiNao Report* at 2 [D.I. 301, Ex. J].

⁴⁸ *JiNao Report* at 19 (emphasis added) [D.I. 301, Ex. J].

⁴⁹ *JiNao Report* at 3 (“A local subsystem is associated with a router/switch to function as a security filter and *analyze the incoming packets* from its neighbors.”), at 5 (“*If a packet passes through the prevention module, it will be forwarded* to the protocol engine for execution and to the local detection module which performs both statistical- and protocol-based intrusion checks), and at 8, 14, 15, 16, 18, 21, 22, 24, 25 [D.I. 301, Ex. J]. *See also* the JiNao System Architecture diagram reproduced *infra* at 54, which shows the JiNao Module receiving input directly from the network.

⁵⁰ *JiNao Report* at 19 (emphasis added) [D.I. 301, Ex. J].

⁵¹ D.I. 301, Ex. J.

⁵² *See* Declaration of L. Todd Heberlein at ¶¶ 4-13.

was unable to “keep the story straight,” necessitating SRI’s three-page attempt to explain away his testimony. And, even then, Dr. Kesidis came to the conclusion that JiNao received network packets: “[JiNao] reacted to packets that are – certain packets that are received by the router. So in the sense that it reacts to those packets, it receives them.”⁵³ SRI’s failure to even address, much less rebut, the disclosures above means the issue is ripe for summary judgment in Defendants’ favor.

2. The JiNao Report anticipates the asserted hierarchical claims

The above discussion regarding “receiving network packets” also dispenses with SRI’s claim that JiNao does not analyze “network traffic data.” Thus, the only remaining limitation in the hierarchical claims that SRI contests is “automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.” Although SRI tries to style its arguments as a debate over whether or not the *JiNao Report* “discloses” this limitation, it, in reality, makes only enablement arguments. Because all of SRI’s enablement arguments are premised on what the JiNao authors *actually built*, which is legally irrelevant, SRI has failed to raise a genuine issue of material fact.

There is no debate that *JiNao Report* actually *discloses* a hierarchical monitor. Figure 1 below illustrates two “Local JiNao” (lower-level monitors) both reporting to a “Remote Management Application” (higher-level monitor).⁵⁴

⁵³ Res. Br. at 28 [D.I. 339]; Compton Decl. Ex. H at 50:16-51:4 [D.I. 340].

⁵⁴ *JiNao Report* at 4 [D.I. 301, Ex. J].

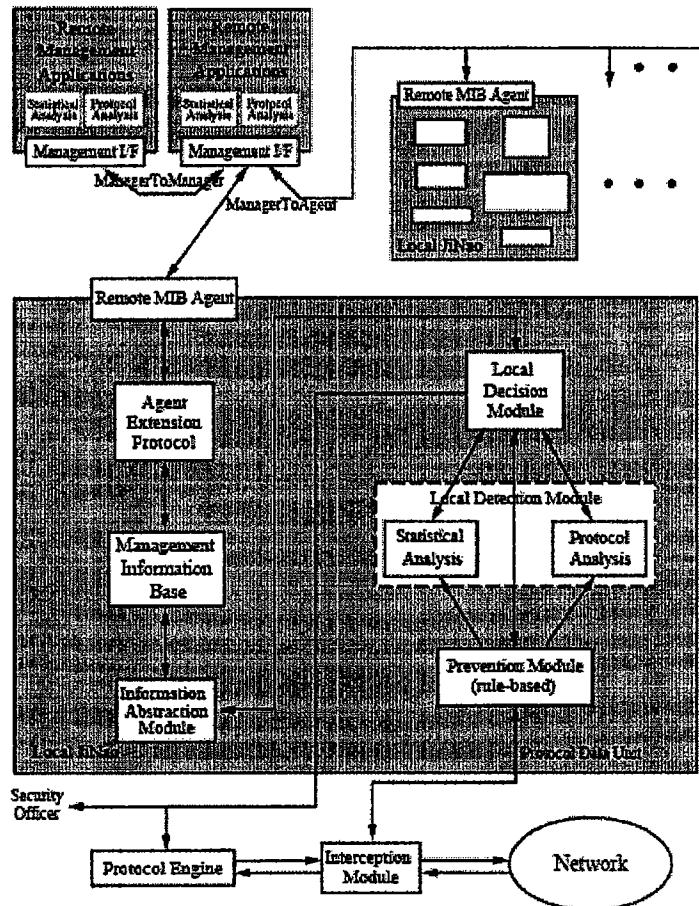


Figure 1: JiNao System Architecture.

The text of the *JiNao Report* also discloses a “scalable architecture” and a “hierarchy” multiple times.⁵⁵

Furthermore, there is no debate that the *JiNao Report* actually *discloses* that the hierarchical monitors “correlate” information from lower-level monitors.⁵⁶ The *JiNao Report* discloses that higher-level monitors correlate information from lower-level monitors in multiple instances, such as:

For example, ... *a higher-level decision module*, i.e. one that has access to observations on a larger topological region, *can correlate multiple detections*

⁵⁵ *JiNao Report* at 3, 7, 13, 29, 31, 32 [D.I. 301, Ex. J]. See also Brown Decl. Ex. M [D.I. 301].

⁵⁶ Because the claims make it clear that “correlation” is a subset of “integration” (see ‘203 claims 1 and 2) if the *JiNao Report* discloses correlation, it necessarily also discloses integration.

from low-levels according to their respective scope of impact, and to reach a more accurate detection decision.⁵⁷

SRI's entire argument regarding the *JiNao* disclosure is premised only on what the *JiNao Report* "teaches and enables."⁵⁸ As "proof" of lack of enablement, SRI relies upon testimony from Mr. Jou, one of the authors of the *JiNao Report*, about what was actually built during the *JiNao* DARPA project.⁵⁹ But "anticipation does not require actual performance of suggestions in a disclosure." *Bristol-Myers Squibb Co. v. Ben Venue Labs., Inc.*, 246 F.3d 1368, 1379 (Fed. Cir. 2001). The Federal Circuit has repeatedly recognized the holding in *In re Donohue*: "It is not ... necessary that an invention disclosed in a publication shall have actually been made in order to satisfy the enablement requirement." *In re Donohue*, 766 F.2d 531, 533 (Fed. Cir. 1985); *see Bristol-Myers Squibb*, 246 F.3d at 1379; *Novo Nordisk Pharma., Inc., v. Bio-Tech. General Corp.*, 424 F.3d 1347, 1355 (Fed. Cir. 2005). Thus, this testimony from Mr. Jou is not relevant.

Furthermore, to the extent that Mr. Jou's testimony suggests that performing "correlation" in *JiNao* was a difficult task, Mr. Jou's testimony also makes it plain that the definition of "correlation" being used by Mr. Jou in making this statement was a far more complex and difficult to implement definition than either parties' definition of "correlation" proposed in this case. According to Mr. Jou:

Correlate means how do you put two or more than two input together and derive meaningful information, or intelligence, out of these different infrastreams of information, and be able to come up with certain rationale or logic that what this, you know, behavior manifests to itself. Probably that's kind of lengthy or wordy, but that's my understanding of this word, correlation.⁶⁰

⁵⁷ *JiNao Report* at 32, *see also* 13, 29, 36 [D.I. 301, Ex. J]. *See also* Brown Decl. Ex. M [D.I. 301].

⁵⁸ Res. Br. at 24 [D.I. 339].

⁵⁹ Res. Br. 23-24 [D.I. 339]; Kesidis Decl. Ex. B at ¶ 27 [D.I. 348].

⁶⁰ Jou Tr. 173 [7/10/06 Godfrey Decl. Ex. UU].

Here, neither party offers a construction of correlation like the sophisticated definition used by Mr. Jou. SRI itself has argued for a broad construction of the limitation “wherein integrating comprises correlating intrusion reports reflecting underlying commonalities” *in the patents-in-suit* as “[c]ombining the reports based on underlying commonalities between them.”⁶¹

This broad, simple definition of “correlation” is necessary because the patents-in-suit do not describe or enable any more complex form of integration or correlation. The specification does not provide any algorithms, logic, or explanation of how integration or correlation is to be performed. Indeed, SRI’s expert conceded that there was no specific example of correlation or integration provided in the preferred embodiment disclosed in the specification.⁶² By contrast, the *JiNao Report* at 35-36⁶³ actually provides an explicit example of a higher-level monitor “Timothy” combining information from two lower-level monitors “Alice” and “Chris” to perform correlation. Thus, the *JiNao Report*’s explicit instruction to “correlate intrusion events among several routers,”⁶⁴ as well as the explicit example provided at pages 35-36 fully enables the “integrating” and “correlating” limitations of the hierarchical patent claims.

III. CONCLUSION

Since the systems and methods claimed in the asserted claims of the ‘338, ‘203, ‘212, and ‘615 patents were described in printed publications more than one year before their date of application for patent, Defendants are entitled to summary judgment pursuant to 35 U.S.C. § 102 and 103 that the claims are invalid as a matter of law.

⁶¹ See Joint Claims Construction Statement [D.I. 174].

⁶² Kesidis Tr. 706-714 at 711 [7/10/06 Godfrey Decl. Ex. SS].

⁶³ D.I. 301, Ex. J.

⁶⁴ *JiNao Report* at 13 [D.I. 301, Ex. J].

Dated: July 10, 2006

POTTER ANDERSON & CORROON LLP

MORRIS, JAMES, HITCHENS &
WILLIAMS, LLP

/s/ David E. Moore

Richard L. Horwitz (#2246)
David E. Moore (#3983)
Hercules Plaza, 6th Floor
1313 N. Market Street
Wilmington, DE 19899
Tel.: (302) 984-6000
Fax: (302) 658-1192

OF COUNSEL:

Holmes J. Hawkins III
Natasha H. Moffitt
KING & SPALDING LLP
191 Peachtree Street
Atlanta, GA 30303
Tel: (404) 572-4600
Fax: (404) 572-5145

Theresa A. Moehlman
KING & SPALDING LLP
1185 Avenue of the Americas
New York, New York 10036
Tel.: (212) 556-2100
Fax: (212) 556-2222

Attorneys for Defendant
INTERNET SECURITY SYSTEMS, INC.,
a Delaware Corporation and
INTERNET SECURITY SYSTEMS, INC.,
a Georgia Corporation

/s/ Richard K. Herrmann

Richard K. Herrmann (#405)
Mary B. Matterer (#2696)
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
Tel.: (302) 888-6800

OF COUNSEL:

Lloyd R. Day, Jr.
Robert M. Galvin
Paul S. Grewal
DAY, CASEBEER MADRID &
BATCHELDER LLP
20300 Stevens Creek Blvd.,
Suite 400
Cupertino, CA 95014
Tel: (408) 873-0110
Fax: (408) 873-0220

Michael J. Schallop
Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
Tel: (408) 517-8000
Fax: (408) 517-8121

Attorneys for Defendant
SYMANTEC CORPORATION

CERTIFICATE OF SERVICE

I hereby certify that on the 19th day of July, 2006, I electronically filed the foregoing document, **REDACTED DEFENDANTS' JOINT REPLY BRIEF IN SUPPORT OF THEIR MOTION FOR SUMMARY JUDGMENT OF INVALIDITY PURSUANT TO 35 U.S.C. §§ 102 & 103**, with the Clerk of the Court using CM/ECF which will send notification of such filing to the following:

John F. Horvath, Esq.
Fish & Richardson, P.C.
919 North Market Street, Suite 1100
Wilmington, DE 19801

Richard L. Horwitz, Esq.
David E. Moore, Esq.
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
Wilmington, DE 19801

Additionally, I hereby certify that on the 19th day of July, 2006, the foregoing document was served via email on the following non-registered participants:

Howard G. Pollack, Esq.
Michael J. Curley, Esq.
Fish & Richardson
500 Arguello Street, Suite 500
Redwood City, CA 94063
650.839.5070

Holmes Hawkins, III, Esq.
King & Spalding
191 Peachtree St.
Atlanta, GA 30303
404.572.4600

Theresa Moehlman, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036-4003
212.556.2100

/s/ Richard K. Herrmann

RICHARD K. HERRMANN (#405)
MARY B. MATTERER (#2696)
Morris, James, Hitchens & Williams LLP
222 Delaware Avenue, 10th Floor
Wilmington, DE 19801
(302) 888-6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com
Counsel for Symantec Corporation